Information Sciences 305 (2015) 285–301

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Punctured interval broadcast encryption scheme with free riders ☆

Murat Ak [a,*], Ali Aydın Selçuk [b]

[a] Dept. of Computer Engineering, Akdeniz University, Antalya, Turkey
[b] Dept. of Computer Eng., TOBB Univ. of Economics and Tech., Ankara, Turkey

ARTICLE INFO

Article history:
Received 17 February 2012
Received in revised form 24 August 2014
Accepted 1 February 2015
Available online 7 February 2015

Keywords:
Broadcast encryption
Free rider
Punctured interval
Digital rights management

ABSTRACT

In Broadcast Encryption (BE) schemes, the problem is to encrypt a content for a group of dynamically changing privileged (subscriber) subset within a receiver population. A popular approach is to carefully distribute a group of keys to several, carefully designed subsets of the receivers beforehand, and later use a precise subset of keys so that only intended users have those keys, thus decrypt the content. This approach is known as the *subset cover framework*. In the subset cover framework, one concern is the number of copies that must be encrypted, which affects the bandwidth requirement. This problem can be relaxed by allowing a limited number of *free riders* so that, by sacrificing some coverage accuracy, the transmission cost is reduced. Several BE schemes are proposed since 90s, and one of the most efficient schemes so far is the punctured interval BE scheme (Cheon et al., 2008). In this paper, we attack the problem of how to assign a given number of free riders effectively in the punctured interval BE scheme. We give the optimal free rider assignment algorithm which runs in $poly(n)$ time, where n is the number of all users in the system, and we provide a heuristic which performs slightly worse than the optimal algorithm in terms of transmission cost reduction but is much faster, i.e., linear in terms of n. We also propose a hybrid approach which employs the core ideas of both optimal and heuristic methods in order to achieve a trade-off between speed and accuracy.

1. Introduction

Broadcast encryption (BE) is a cryptographic primitive for broadcasting digital content to a large set of receivers where only a *dynamically changing* authorized subset is eligible to decrypt it. The usage of BE ranges from protecting recordable digital content in multimedia applications such as pay-TV, secure audio/video streaming and Internet multicasting, to file system security. Basically, whenever access control needs to be imposed on a one-way communication channel, BE is good alternative to employ. This key role of BE makes it a useful tool in digital rights management (DRM) technology. BE schemes are typically realized by embedding a set of long-term keys into the receiver devices before their purchase. When a broadcast is to be made later, these keys are used to encrypt the data according to the subscriber set of the current broadcast.

In different settings, some concerns such as user domain size, security, bandwidth, or hardware may be more important than others. However, usually, two concerns are inherent in almost all BE systems. First, the amount of key storage must be

☆ This work was supported in part by the Turkish Scientific and Technological Research Agency (TÜBİTAK), under grant number 111E213.
* Corresponding author.
E-mail addresses: muratak@akdeniz.edu.tr (M. Ak), aselcuk@etu.edu.tr (A.A. Selçuk).

http://dx.doi.org/10.1016/j.ins.2015.02.001
0020-0255/

adequate because the long-term secure storage size at the receiver side is very limited since it has to be tamper resistant. Second, the amount of additional data sent along with the content through the communication channel, called the transmission overhead, must be adequate because of the limited nature of the bandwidth of communication channels.

Note that for communication channels that are two-way, more effective solutions than embedding long-term keys are possible. However, most of the broadcasting communication channels are typically one way, such as satellite channels, and the user decoders are modeled as stateless, meaning that they have no typical long-term memory.

There are two basic evaluation parameters common in BE systems: One is called the *key storage* and the other is called the *transmission overhead* of a broadcast. In 2001, in their seminal paper, Naor et al. [20] proposed the subset difference (SD) scheme which became the most efficient scheme at that time. Then its variants [12,13] are proposed in order to gain improvement by adding layers. The SD scheme has since become popular and it is implemented in the next-generation DVD standard [1].

Despite this popularity, the SD scheme did not long remain as the most efficient scheme. Jho et al. [8] proposed a combination of three schemes, which offers better performance compared to the SD scheme. The punctured interval (PI) was one of these schemes offered [8]. PI scheme considers users on a hypothetical line, and subsets are designed as special intervals on this line possibly with a limited number of punctures (gaps).

In all traditional BE schemes, by default, it is assumed that all unauthorized receivers must be revoked in an encrypted broadcast. However, Abdalla et al. [2] pointed out that this assumption could be relaxed for some applications, and the transmission overhead can be reduced significantly by allowing a limited amount of free riders. In this case, there needs to be a limit on the number of free riders allowed, and the question is how to optimally use this given free rider quota. Note that we do not claim all BE schemes can allow free riders and enjoy the performance gain. This idea is only applicable if the broadcast content does not need to stay strictly confidential against anyone outside the intended recipients.

1.1. Related work

The idea of BE is introduced by Berkovits [5] in 1991. However the model of Fiat and Naor [11] is celebrated to be the first formal model of BE. They introduced the *resiliency* concept for BE, and called a scheme *k-resilient* if it is secure against any k revoked users working together, so that they would not be able to decrypt the encrypted broadcast message. They also described a scheme that required every receiver to store $O(k \log k \log n)$ keys and the center to broadcast $O(k^2 \log^2 k \log n)$ messages where n is the total number of users. Later on, fully resilient schemes dominated the BE research and these schemes became obsolete.

In 1999, the logical key hierarchy (LKH) was proposed independently by Wallner et al. [23] and Wong et al. [24]. According to LKH, the receivers were being associated with the leaves of a tree, and a unique key is associated with each node of the tree. Then, each receiver is given the keys of the nodes on the path from the corresponding leaf to the root. Although being originally proposed for secure Internet multicast, LKH was quite useful for BE. Recognizing this fact, Abdalla et al. [2] used LKH to design a BE scheme and reduced key storage complexity to logarithmic scale in terms of the number of receivers, namely to $O(\log n)$ while achieving $O(n)$ transmission overhead.

In their seminal paper, [20], Naor et al. proposed the renowned subset difference (SD) scheme. The SD scheme decreased the transmission overhead to $O(r)$ while keeping the key storage $O(\log^2 n)$ by employing one-way functions. Later two important variants of SD was proposed. The layered subset difference (LSD) scheme, which was proposed by Halevy and Shamir [13]. Their optimized LSD scheme has a transmission overhead of $O(\log n \log\log n)$ and a key storage of $O(r \log\log n)$. Goodrich et al. [12] introduced the stratified subset difference (SSD) scheme, which has $O(r \log n/\log\log n)$ transmission overhead and $O(\log n)$ key storage complexity. Horwitz presented an analysis of [11,13,20] in his survey [14].

In 2005, Jho et al. [8] proposed the Punctured Interval (PI) scheme. The PI scheme is also a subset cover framework scheme but with a different subset structure. The subsets are designed as intervals with possible skippings on a straight line on which users are thought to be placed virtually. Originally, in [17,16,8,15], the PI scheme is employed alongside two other subset cover schemes called C-basic chain and cascade chain and they are treated as one combined scheme. Basic chain subsets are defined as all intervals with a length less than a bound. On top of the basic chain and PI subsets, these schemes also employ the cascading idea to bring extra transmission cost efficiency by grouping subsets from different layers together. This combined scheme outperforms the SD scheme in terms of transmission overhead but with a slightly larger key storage requirement.

In 2008, Austrin and Kreitz [4] gave lower bounds for the transmission costs for many broadcast encryption schemes in the subset cover framework which includes the ones that use pseudorandom number generators in key distribution phase. They showed that in case where the number of privileged users is small, $O(n - r)$ encryptions are needed which means that there is no strategy which is asymptotically better than assigning each user a different key. Since PI is a scheme of this kind, we do not focus on the few privileged users case.

On the other hand, a number of different approaches to the BE problem have been introduced in the public key setting. Typically, these schemes rather depend on number theoretic structures and there are no predefined subsets. They allow keys to be generated on-the-fly for any privileged user subset. In 2005, Boneh et al. [6] used bilinear maps and the bilinear decision Diffie–Hellman exponent problem to design a public key BE system. Their scheme has constant size private key and offers a trade-off between ciphertext and public key sizes, product of which can be linear in the number of receivers.